FinxS System – Security Statement

To: Person, Organization

European Union General Data Protection Regulation (GDPR)

In 1980, in an effort to create a comprehensive data protection system throughout Europe, the Organization for Economic Cooperation and Development (OECD) issued its "Recommendations of the Council Concerning Guidelines Governing the Protection of Privacy and Trans-Border Flows of Personal Data". The seven principles governing the OECD's recommendations for protection of personal data were:

1.Notice—data subjects should be given notice when their data is being collected;
2.Purpose—data should only be used for the purpose stated and not for any other purposes;
3.Consent—data should not be disclosed without the data subject's consent;
4.Security—collected data should be kept secure from any potential abuses;
5.Disclosure—data subjects should be informed as to who is collecting their data;
6.Access—data subjects should be allowed to access their data and make corrections to any inaccurate data; and
7.Accountability—data subjects should have a method available to them to hold data collectors accountable for not following the above principles.

In January 2012, the European Commission proposed a comprehensive reform of data protection rules in the EU. The completion of this reform is a policy priority for 2015. The objective of this new set of rules was to give citizens back control over of their personal data, and to simplify the regulatory environment for business. The data protection reform was a key enabler of the Digital Single Market which the Commission has prioritized. The reform was to allow European citizens and businesses to fully benefit from the digital economy.

On 27 April 2016 The European Parliament and the Council decided on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) to be in effect on 25 May 2018.

Under GDPR, personal data can only be gathered legally under strict conditions, for a legitimate purpose. Furthermore, persons or organizations which collect and manage personal information must protect it from misuse and must respect certain rights of the data owners which are guaranteed by EU law.

Data may be processed only under the following circumstances. (art. 7):

- when the data subject has given their consent.
- when the processing is necessary for the performance of or the entering into a contract.
- when processing is necessary for compliance with a legal obligation.
- when processing is necessary in order to protect the vital interests of the data subject.
- processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller or in a third party to whom the data are disclosed.
- processing is necessary for the purposes of the legitimate interests pursued by the controller or by the third party or parties to whom the data are disclosed, except where such interests are overridden by the interests for fundamental rights and freedoms of the data subject. The data subject has the right to access all data processed about him. The data subject even has the right to demand the rectification, deletion or blocking of data that is incomplete, inaccurate or isn't being processed in compliance with the data protection rules. (art. 12)

To protect the rights and freedom of an individual (data subject), the data subject has been assigned certain rights:

- Right of access by the data subject (The data subject shall have the right to obtain from the controller confirmation as to whether or not personal data concerning him or her are being processed, and, where that is the case, access to the personal data) – art 15
- Right to rectification (The data subject shall have the right to obtain from the controller without undue delay the rectification of inaccurate personal data concerning him or her. Taking into account the purposes of the processing, the data subject shall have the right to have incomplete personal data completed, including by means of providing a supplementary statement.) – 1rt 16

- Right to erasure ('right to be forgotten') (The data subject shall have the right to obtain from the controller the erasure of personal data concerning him or her without undue delay and the controller shall have the obligation to erase personal data without undue delay) – art 17
- Right to restriction of processing (The data subject shall have the right to obtain from the controller restriction of processing) – art 18
- Right to data portability (The data subject shall have the right to receive the personal data concerning him or her, which he or she has provided to a controller, in a structured, commonly used and machine-readable format and have the right to transmit those data to another controller without hindrance from the controller) – art 20
- Right to object and automated individual decision-making (The data subject shall have the right to object, on grounds relating to his or her particular situation, at any time to processing of personal data concerning him or her) – art 21
- Automated individual decision-making, including profiling (The data subject shall have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her.) – art 22

Data Protection Policy

Data protection policy defines the goals, principles, responsibilities and implementation of data protections during the time data is stored on FinxS System. Data protection policy complies with European Union and local legislation.

FinxS Oy Ltd assumes all its partners within European Union align with and commit themselves to complying with the same data protection policy.

High data protection is crucially important for the continuity of the business of FinxS Oy Ltd. FinxS System is used by large amount of clients from all around the world and we must guarantee the protection of their data to best reasonably possible level. Our aim is to guarantee the availability of our services in all situations. Most of the details in data protection are classified information either due to security reasons or requirements by legislation.

The main principles in data protection are:

- Data availability and usability (those who are entitled to access the data should be able to do it without unnecessary delay)
- Data confidentiality (data is accessed only be persons who have rights to the data)
- Data consistency (there are no unauthorized editions to the data and it has not been changed due to irregular errors)
- Data non-repudiation (owner or provider of the data cannot deny providing the data)

The purpose of the data protection policy is to:

- Guarantee the trust of the user of the FinxS System
- Fulfill all legal obligations
- Guarantee the continuity of the business
- Guarantee the continuity of the production

Data Security Policy

Maintaining data security is an integral part of the business of FinxS Oy Ltd. It is closely connected with data protection and defines in more detail how in different elements of the FinxS System the data security and rights for data subjects are lawfully covered,

Processing personal data
Processing personal data is based on the consent of the data subject and other grounds defined by law. Data can be processed only be persons who need the data in completing their duties and only to the extent required for that. Personal data is processed only for the purpose they were originally collected for, unless otheriwse agreed with the data subject. Personal data can be given to third parties only with permission from the data subject or as required by law. Personal data is stored only as long as needed for the purpose they were collected for or longer if required ny law or other obligations.

Efforts are made to guarantee the correctness of the data. Data is updated hwen needed, based on information received from the data subject or other reliable sources. When data is no more needed and also not needed to store by law, it will be removed with appropriate measures.

Responsibility of data protection is held by for whom the data is originally collected for. Every person involved needs to be aware and manage the data protection and risks concerned. Data processing is controlled by law and good practices. including being responsible for one's actions.

Personal data is stored in FinxS System or systems that FinxS Oy Ltd has sub-contracted from. Non-authorized persons do not have access to the system nor are they given any information without consent from data subject.

Rights of data subject
Data subject has the right to check and correct information concerning him/her. Data subject has also (as detailed by law) the right to ask for their data to be removed, limit the processing of the data, and right to transfer the data to another data processor.

Server location
FinxS System Servers are located within European Union. They shall not be moved from EU/EEA without prior written consent of the users.

Server communication
FinxS System Servers are protected against unauthorized access. They use a SSL Certificate to ensure secured internet communication (https protocol). All communication between FinxS and client browser is encrypted. The server has regularly updated firewall and virus protection.

Email security
FinxS System allows users to encrypt email attachment that contain assessment reports of data subject. Passwords are defined and known only be users and can be different for each data collection project.

Development software
All development and maintenance software is updated regularly. All available security fixes are applied immediately.

System software
System software is updated regularly. All available security fixes are applied immediately. Error tracking software is in place to detect any user experienced problems and server-side errors to enable fixing them immediately.

Contingency plan
FinxS System's database is replicated in multiple locations. The possible need to take a back-up copy in use is well documented and the documents are updated annually together with all security policies.

Logs
System keeps log on all main activities to protect the rights of data subjects. Among other activities, logs are created for API communication by client servers, failed login attempts, succeeded and failed data collection, users logins, possibility of different entities to access personal data, deleting of personal data and system errors.

Data breach policy
In case of known or suspected data breach, the entities the data breach may affect will be notified without undue delay and as required by GDPR.

User access
Login to the data collection features of FinxS System is protected by Access Code and Password, and is controlled by the administrative user. Separate login procedure exists for the administration features. The passwords are changed regularly. Users are routinely informed about the risks of not changing their personal passwords. The login time to the system is time limited.

Physical premises
Entry to the building is protected by password control. Entrance is allowed only by registration and acceptance by a contact person. The route to the engine room is controlled by movement detection system and recording cameras.

Entry to the engine room is only possible when escorted by a staff member. All visits are to be agreed beforehand. The identity of each person entering the room is checked. The engine room is air conditioned, humidity controlled and power supply is protected by UPS system. Fire plan is accepted by the local fire department and emergency fire system is in place and does not cut off server power supply when in use. 24/7 support center that monitors the server room. External security service is acquired to protect access to the building.

Server room is audited, among other, to be PCI-DSS compatible and the service provider has given ISO 27001 - certificate.

Data connections
All data connections are doubled by using different physical routes and locations. Data is secured by replicated back-up system.

System downtime
Normal system updates do not require system downtime. Operating system updates may require this, but they are limited to no longer than 1% of time. FinxS cannot control force majeure downtimes caused by reasons beyond its control.

Privacy statement
FinxS Oy Ltd is committed to secure all its customers privacy and provide secure and safe solutions. Trustworthy computing under all circumstances is the leading guideline for operations. No compromises need to be taken nor are shortcuts in security controls tolerated.

All user information is confidential. FinxS Oy Ltd will always conform to legal requirements and will never sell, share or hand out any sensitive or personal information of our customer.

Policies, processes, procedures, responsibilities, guidelines and reporting are periodical reviewed and if necessary updated as part of standard operational duties.

Security Vulnerability Disclosure Policy
If you believe you have found a security vulnerability on Nebula website or service, we encourage you to let us know right away by reporting to info@finxs.com. We will investigate all legitimate reports and do our best to quickly fix the problem. Before reporting though, please review this page including our responsible disclosure policy, reward guidelines, and those things that should not be reported.

Responsible Disclosure Policy

If you comply with the policies below when reporting a security issue to FinxS Oy Ltd, we will not initiate a lawsuit or law enforcement investigation against you in response to your report. We ask that:
• You give us reasonable time to investigate and mitigate an issue you report before making public any information about the report or sharing such information with others.
• You make a good faith effort to avoid security violations and disruptions to FinxS System and services, including (but not limited to) destruction of data and interruption or degradation of our services.
• You do not exploit a security issue you discover for any reason. (This includes demonstrating additional risk or probing for additional issues.)
• You do not violate any other applicable laws or regulations.

For more detailed information, please contact info@finxs.com.

***
We follow the recommendations, policies and law set by the European authorities. We also assume our partners comply with the law and regulations, and we only work with partners who commit themselves to these same principles.

April 10th, 2018

FinxS Oy Ltd